REMARKS

Claims 1-60 were pending in the application. Claims 1-60 were rejected. Claims 1 and 21 are canceled without prejudice to or disclaimer of the subject matter recited therein. Claims 2-4, 6, 7, 22-24, 26, 27, 41, 43-45, 51, and 53-55 are amended. Claims 2-20 and 22-60 are now pending in the application. Claims 6, 7, 26, and 27 are the independent claims. Reconsideration of the amended application is respectfully requested.

The examiner rejected claims 1-60 under the judicially-created doctrine of obviousness-type double patenting as being unpatentable over claims 1-65 of U.S. Patent No. 6,885,747. Independent claims 6, 7, 26, and 27 each include the limitation that the key splits are combined on a smart card. The cited reference does not disclose or suggest this feature, and therefore could not have claimed this feature. For at least this reason, it is submitted that the instant claims are patentably distinct from those of the cited reference. The rejection, therefore, should be withdrawn.

The examiner rejected claims 1-60 under the judicially-created doctrine of obviousness-type double patenting as being unpatentable over claims 1-67 of U.S. Patent No. 6,542,608. Independent claims 6, 7, 26, and 27 each include the limitation that the key splits are combined on a smart card. The cited reference does not disclose or suggest this feature, and therefore could not have claimed this feature. For at least this reason, it is submitted that the instant claims are patentably distinct from those of the cited reference. The rejection, therefore, should be withdrawn.

The examiner rejected claims 1-60 under the judicially-created doctrine of obviousness-type double patenting as being unpatentable over claims 1-67 of U.S. Patent No. 6,549,623. Independent claims 6, 7, 26, and 27 each include the limitation that the key splits are combined on a smart card. The cited reference does not disclose or suggest this feature, and therefore could not have claimed this feature. For at least this reason, it is submitted that the instant claims are patentably distinct from those of the cited reference. The rejection, therefore, should be withdrawn.

The examiner rejected claims 1-60 under the judicially-created doctrine of obviousness-type double patenting as being unpatentable over claims 1-35 of U.S. Patent No. 6,608,901. Independent claims 6, 7, 26, and 27 each include the limitation that the key splits are combined on a smart card. The cited reference does not disclose or suggest this feature, and therefore could not have claimed this feature. For at least this reason, it is submitted that the instant claims are patentably distinct from those of the cited reference. The rejection, therefore, should be withdrawn.

The examiner rejected claims 1-60 under the judicially-created doctrine of obviousness-type double patenting as being unpatentable over claims 1-62 of U.S. Patent No. 6,606,386. Independent claims 6, 7, 26, and 27 each include the limitation that the key splits are combined on a smart card. The cited reference does not disclose or suggest this feature, and therefore could not have claimed this feature. For at least this reason, it is submitted that the instant claims are patentably distinct from those of the cited reference. The rejection, therefore, should be withdrawn.

The examiner rejected claims 1-6 and 21-26 under 35 USC §102(e) as being anticipated by Morgan et al.

Claim 6 is amended into independent form, including all of the limitations of base claim 1, which is canceled. As amended, claim 6 recites a method of encrypting an object. According to the recited method, a plurality of key splits is combined to generate a cryptographic key. A cryptographic algorithm is initialized with the cryptographic key. The initialized cryptographic algorithm is applied to the object, to form an encrypted object. At least one of the plurality of key splits corresponds at least in part to a biometric measurement. Combining the plurality of key splits to generate the cryptographic key is performed on a smart card.

Morgan et al. disclose a security method and system for persistent storage and communications on computer network systems. Morgan et al. disclose split symmetric persistent storage keys PK1 and PK2 that are combined to yield a persistent storage key PK. Each split can be generated by any of a number of different means, as disclosed by Morgan et al., including by reading biometric data, or by reading a token corresponding to the key split from a pre-encoded smart card. See column 14, lines 20-43. However, Morgan et al. do not disclose or suggest that the key splits are combined on the smart card in order to generate the key, as recited in claim 6. Rather, Morgan et al. only disclose that key splits can be derived from a smart card, and do not disclose or suggest any advantage to combining the key splits on a smart card.

For at least the reasons noted above, it is submitted that Morgan et al. do not anticipate the invention recited in claim 6. Claims 2-5 depend from claim 6, and therefore also are not anticipated by Morgan et al. The rejection of claims 2-6, therefore, should be withdrawn.

Claim 26 is amended into independent form, including all of the limitations of base claim 21, which is canceled. As amended, claim 26 recites a storage medium that includes instructions for causing a data processor to encrypt an object. The instructions include generate a cryptographic key by combining a plurality of key splits, initialize a cryptographic algorithm with the cryptographic key, and apply the initialized cryptographic algorithm to the object to form an encrypted object. At least one of the key splits corresponds at least in part to a biometric measurement. The data processor is distributed, and the instruction to generate a cryptographic key is executed at least in part on a smart card.

Morgan et al. disclose a security method and system for persistent storage and communications on computer network systems. Morgan et al. disclose split symmetric persistent storage keys PK1 and PK2 that are combined to yield a persistent storage key PK. Each split can be generated by any of a number of different means, as disclosed by Morgan et al., including by reading biometric data, or by reading a token corresponding to the key split from a pre-encoded smart card. See column 14, lines 20-43. However, Morgan et al. do not disclose or suggest that the key splits are combined on the smart card in order to generate the key, as recited in claim 26. Rather, Morgan et al. only disclose that key splits can be derived from a smart card, and do not disclose or suggest any advantage to combining the key splits on a smart card.

For at least the reasons noted above, it is submitted that Morgan et al. do not anticipate the invention recited in claim 26. Claims 22-25 depend from claim 26, and therefore also are not anticipated by Morgan et al. The rejection of claims 22-26, therefore, should be withdrawn.

The examiner rejected claims 1-3, 7-23, and 27-60 under 35 USC §102(e) as being anticipated by Scheidt et al.

Claim 6 is amended into independent form, including all of the limitations of base claim 1, which is canceled. As amended, claim 6 recites a method of encrypting an object. According to the recited method, a plurality of key splits is combined to generate a cryptographic key. A cryptographic algorithm is initialized with the cryptographic key. The initialized cryptographic algorithm is applied to the object, to form an encrypted object. At least one of the plurality of key splits corresponds at least in part to a biometric measurement. Combining the plurality of key splits to generate thc cryptographic key is performed on a smart card.

Scheidt et al. disclose a cryptographic key split combiner that accepts key splits generated from seed values and combines the splits to form a cryptographic key. However, Scheidt et al. do not disclose or suggest that the key splits are combined on the smart card in order to generate the key, as recited in claim 6, nor do Scheidt et al. disclose or suggest any advantage to combining the key splits on a smart card.

For at least the reasons noted above, it is submitted that Scheidt et al. do not anticipate the invention recited in claim 6. Claims 1-3 and 41-45 depend from claim 6, and therefore also are not anticipated by Scheidt et al. The rejection of claims 1-3 and 41-45, therefore, should be withdrawn.

Independent claim 7, as amended, recites a method of encrypting an object by a user, in a cryptographic system associated with an organization. According to the claimed method, a first cryptographic key is generated by combining, on n smart card, an organization split corresponding to the organization, a maintenance split, a random split, a biometric split corresponding to the user, and at least one label split. A cryptographic algorithm is initialized with the first cryptographic key. The object is encrypted according to the initialized cryptographic algorithm. Combiner data is added to the encrypted object. The combiner data includes reference data corresponding to at least one of the at least one label split and the cryptographic algorithm, name data associated with the organization, the maintenance split and/or a maintenance level associated with the maintenance split, and the random split. The encrypted object is stored with the added combiner data.

Scheidt et al. disclose a cryptographic key split combiner that accepts key splits generated from seed values and combines the splits to form a cryptographic key. However, Scheidt et al. do not disclose or suggest that the key splits are combined on the smart card in order to generate the key, as recited in claim 7, nor do Scheidt et al. disclose or suggest any advantage to combining the key splits on a smart card.

For at least the reasons noted above, it is submitted that Scheidt et al. do not anticipate the invention recited in claim 7. Claims 8-20 and 46-50 depend from claim 7, and therefore also are not anticipated by Scheidt et al. The rejection of claims 7-20 and 46-50, therefore, should be withdrawn.

Claim 26 is amended into independent form, including all of the limitations of base claim 21, which is canceled. As amended, claim 26 recites a storage medium that includes instructions for causing a data processor to encrypt an object. The instructions include generate a cryptographic key by combining a plurality of key splits, initialize a cryptographic algorithm with the cryptographic key, and apply the initialized cryptographic algorithm to the object to form an encrypted object. At least one of the key splits corresponds at least in part to a biometric measurement. The data processor is distributed, and the instruction to generate a cryptographic key is executed at least in part on a smart card.

Scheidt et al. disclose a cryptographic key split combiner that accepts key splits generated from seed values and combines the splits to form a cryptographic key. However, Scheidt et al. do not disclose or suggest that the key splits are combined on the smart card in order to generate the key, as recited in claim 26, nor do Scheidt et al. disclose or suggest any advantage to combining the key splits on a smart card.

For at least the reasons noted above, it is submitted that Scheidt et al. do not anticipate the invention recited in claim 26. Claims 21-23 and 51-55 depend from claim 26, and therefore also are not anticipated by Scheidt et al. The rejection of claims 21-23 and 51-55, therefore, should be withdrawn.

Independent claim 27, as amended, recites a storage medium comprising instructions for causing a data processor to encrypt an object. The instructions include generate a first cryptographic key by combining, on a smart card, an organization split corresponding to an organization, a maintenance split, a random split, a biometric split corresponding to the user, and at least one label split; initialize a cryptographic algorithm with the first cryptographic key; apply the initialized cryptographic algorithm to the object to form an encrypted object; add combiner data to the encrypted object and store thc encrypted object with the combiner data for subsequent access. The combiner data includes reference data corresponding to at least one of the at least one label split and the cryptographic algorithm, name data associated with the organization, at least one of the maintenance split and a maintenance level corresponding to the maintenance split, and the random split.

Scheidt ct al. disclose a cryptographic key split combiner that accepts key splits generated from seed values and combines the splits to form a cryptographic key. However, Scheidt et.al. do not disclose or suggest that the key splits are combined on the smart card in order to generate the key, as recited in claim 27, nor do Scheidt et al. disclose or suggest any advantage to combining the key splits on a smart card.

For at least the reasons noted above, it is submitted that Scheidt et al. do not anticipate the invention recited in claim 27. Claims 28-40 and 56-60 depend from claim 27, and therefore also are not anticipated by Scheidt et al. The rejection of claims 27-40 and 56-60, therefore, should be withdrawn.

Based on the foregoing, it is submitted that all objections and rejections have been overcome. It is therefore requested that the Amendment be entered, the claims allowed, and the case passed to issue.

Respectfully submitted,

February 27, 2006
Date

Thomas M. Champagne
Registration No. 36,478
Customer Number 49691
(828) 253-8600

TMC:hlp